

I QUATTRO PROBLEMI ADDITIVI CLASSICI LE NOSTRE SOLUZIONI E CONSIDERAZIONI

Gruppo ERATOSTENE

.....

Qualche studioso dei numeri primi si fa delle domande su possibili relazioni tra i problemi additivi (per es. Goldbach) e i problemi moltiplicativi (per es. fattorizzazione). Ne citeremo soltanto due, per poi rispondere con nostre considerazioni e proposte di soluzione.

1) Prof. Peter Atkins, nel suo ottimo e recente libro “Il dito di Galileo - Le dieci grandi idee della scienza” (Raffaello Cortina Editore, 2004) pag. 409:

“ La congettura di Goldbach non è stata ancora dimostrata, a dispetto di molti sforzi. La difficoltà sembrerebbe nascere dal fatto che i primi emergono dal concetto di moltiplicazione, ma vengono invocati qui nel contesto dell’addizione. Ad ogni modo, questa congettura potrebbe esemplificare una caratteristica che tra non molto vedremo salire al centro della ribalta: è pure possibile che non esista alcuna dimostrazione, e nemmeno si dia dimostrazione della sua negazione. Goldbach congetturò pure che ogni numero dispari (nota come ipotesi debole di Goldbach, N.d.A.A.) sia la somma di tre primi. Questa congettura è stata parzialmente dimostrata nel 1937

(la dimostrazione funziona solo con numeri molto grandi) dal matematico russo Ivan Matveyedich Vinogradov (1891 – 1983).”

Commento: anche noi abbiamo trattato questa ipotesi, nota come Ipotesi debole di Goldbach, in “Procedure per la formazione delle coppie di Goldbach e delle terne di Goldbach”, sul nostro sito www.gruppoeratostene.com in sezione “Articoli su Goldbach”.

La nostra trattazione dell’ipotesi debole non richiede affatto i grandi numeri di Vinogradov, ma funziona anche con numeri piccoli, a partire dal numero minimo $7 = 2 + 2 + 3$, così come per Goldbach forte il numero minimo è $4 = 2+2$; richiede però la dimostrazione di Goldbach forte, che si trova anch’essa nella suddetta sezione del nostro sito (con il titolo “Proposta di dimostrazione del teorema di Goldbach”).

Infatti, se si aggiunge un numero primo ad un numero pari, già somma di due numeri primi, abbiamo un numero dispari N somma di tre numeri primi; noi dimostriamo, e con ciò anche la congettura debole di Goldbach, che tutti i numeri dispari maggiori di 7 sono scrivibili come somma di tre primi, e anche diverse volte al crescere di N dispari, e con meno ripetizioni

o nessuna ripetizione di ciascuno dei tre numeri primi coinvolti:

in sintesi, un numero pari $P \geq 4$, (già somma di due numeri primi)

più un numero primo qualsiasi $p > 2$, dà un numero dispari N

somma di tre numeri primi, infatti $P = p' + p$ e quindi

$$P + p = N = p' + p + p = \text{somma di tre primi.}$$

Per esempio:

$$N = 19 = 16 + 3 = 11 + 5 + 3 \text{ nessuna ripetizione}$$

$$N = 19 = 16 + 3 = 13 + 3 + 3 \text{ una ripetizione di 3}$$

$$N = 19 = 14 + 5 = 7 + 7 + 5 \text{ una ripetizione di 7}$$

$$N = 19 = 12 + 7 = 5 + 7 + 7 \text{ una ripetizione di 7}$$

$$N = 19 = 8 + 11 = 3 + 5 + 11 \text{ nessuna ripetizione}$$

(ma equivalente a $19 = 16 + 3$)

$$N = 19 = 6 + 13 = 3 + 3 + 13 \text{ una ripetizione di 3}$$

(ma equivalente a $19 = 16 + 3$)

Quindi, il numero $N = 19$ è già ben quattro volte la somma di tre numeri primi, senza ripetizioni o con qualche ripetizione, e più cresce N , maggiori sono le possibilità che sia somma di tre numeri primi. Tale dimostrazione può essere estesa anche ad N pari

come somma di k primi con k pari, con numero minimo $n = 2k$,
e ad N dispari come somma di $k+1$ primi, con $k+1$ dispari, e con
numero minimo $n = 2k + 1$ (nella congettura forte, $k = 2$ e
numero primo numero minimo $n = 2 * k = 2 * 2 = 4$, mentre nella
congettura debole $k = 3$ e numero minimo

$$n = 2*k + 1 = 2*3 + 1 = 6 + 1 = 7).$$

Anche la congettura debole, quindi, può ritenersi dimostrata
ed estesa a k primi, il ch  ha richiesto, come abbiamo visto, la
dimostrazione della congettura forte di Goldbach, che   proprio
uno dei quattro problemi classici additivi che vedremo meglio
tra poco, insieme alle nostre soluzioni positive per tutti e quattro.

2) Anche il Prof. Alessandro Languasco e il Prof. A. Perelli
fanno osservazioni simili nel loro articolo web “Numeri primi e
crittografia”(sul sito di Pristem Matematica) la stessa cosa:

“...Concludiamo il paragrafo osservando che in tali problemi
insorgono difficolt  di varia natura; ad esempio, la difficolt 
fondamentale dei problemi 3) e 4) risiede nel fatto che i numeri primi
sono definiti mediante propriet  moltiplicative, mentre i problemi in
questione coinvolgono propriet  additive.”

Insomma, le stesse cose che diceva il prof. Atkins. Detto per
inciso, ricordiamo che l’Universit  di Genova ha in corso un

progetto di ricerca matematica (PRIN) che comprende anche tali problemi additivi. E che sono (dal suddetto articolo dei professori Languasco e Perelli, pubblicato anche su “Matematica e cultura 2000”, Venice 1999, Ed. by M Emmer, Sringer Verlag Italia, 2000, 227-233), i seguenti:

- 1) (primi rappresentati da polinomi) esistono infiniti interi n per cui $n^2 + 1$ è un numero primo? (o più in generale, $P(n)$ è un numero primo per infiniti n , con $P(x)$ polinomio irriducibile senza divisori fissi?)
- 2) (distanza tra due numeri primi consecutivi) esiste sempre un numero primo tra due quadrati perfetti consecutivi?
- 3) (primi gemelli) esistono infiniti numeri primi p tali che $p + 2$ è ancora primo?
- 4) (congettura di Goldbach) ogni intero pari maggiore di 2 può essere scritto come somma di due numeri primi?”

Premesso che consideriamo possibile una connessione tra qualcuno dei suddetti problemi additivi e qualche problema moltiplicativo (per es. congettura di Riemann o la fattorizzazione), e che approfondiremo probabilmente nei prossimi anni (date le difficoltà dell’argomento), la nostra risposta a tutti e quattro i problemi additivi elencati dai Proff. Languasco e Perelli, è affermativa, ed ecco le nostre proposte

di soluzioni positive:

1) $n^2 + 1$ può essere numero primo se e solo se è anche di forma $6k \pm 1$.

Ecco i numeri primi di forma $n^2 + 1$ e anche di forma $6k \pm 1$ (tranne il numero 2) fino a 1000:

n $n^2 + 1$ = $6k \pm 1$ = Numero primo

1	2	$6 * 1 - 4$	2
2	5	$6 * 1 - 1$	5
4	17	$6 * 3 - 1$	17
6	37	$6 * 6 + 1$	37
10	101	$6 * 17 - 1$	101
14	197	$6 * 33 - 1$	197
16	257	$6 * 43 - 1$	257
20	401	$6 * 67 - 1$	401
24	577	$6 * 96 + 1$	577
26	677	$6 * 113 - 1$	677
...

Poiché fino a 100 ci sono 5 primi di forma $n^2 + 1$,

e 25 numeri primi = $\pi(100)$, e fino a 1000 ce ne sono 10, e 168

numeri primi = $\pi(1\ 000)$, il numero r di forma $n^2 + 1$ è

all'incirca *la radice quadrata* del numero di numeri primi fino

a N , e cioè $\pi(N)$:

$$r \sim \sqrt{\pi(N)}$$

$$5 = \sqrt{\pi(100)} = \sqrt{25}$$

$$10 \approx \sqrt{\pi(1\ 000)} = \sqrt{168} = 12,96$$

...

e poiché infine r cresce con $\pi(N)$ e quindi con N che è infinito, ci sono infiniti n tali che n^2+1 sia primo.

Se tale formula matematica fosse valida anche per $N = 10\ 000$, ed essendo $\pi(10\ 000) = 1\ 229$, r sarebbe circa

$$r \approx \sqrt{1\ 229} = 35$$

Essendo N insieme infinito, r è un sottoinsieme altrettanto infinito, poiché cresce in modo direttamente a n e quindi ad N , e quindi anche i numeri n necessariamente pari che soddisfano la condizione $n^2+1 =$ numero primo, sono infiniti.

Una breve e più semplice soluzione di questo problema si trova sull'articolo "Congetture sui numeri primi ancora aperte - Le nostre soluzioni e le loro possibili e utili conseguenze: RSA, RH)" sul nostro sito (Sezione "Articoli su Goldbach", insieme ai tre lavori sulle progressioni aritmetiche di numeri primi (PAP), in sezione "Articoli sulle Progressioni" nei quali si parla anche dei numeri primi, dei primi gemelli e

degli ultimi risultati di Goldston, Yildirim e Pintz.

Lavori che rendono almeno in parte conto del perché ci sono ciclicamente degli intervalli numerici di uguale lunghezza (per es. 100 unità) ma più o meno densi di numeri primi rispetto agli intervalli precedente o successivo a quello considerato.

C'entrano i numeri gemelli (con differenza minima $d=2$ tra due numeri primi consecutivi, ma anche la congettura di Polignac $d = 2n > 2$ tra due numeri consecutivi, che abbiamo in corso di dimostrazione, potrebbe avere la sua importanza per questo problema (vedi anche problema n° 3).

2) (distanza tra due numeri primi consecutivi) esiste sempre un numero primo tra due quadrati perfetti consecutivi?

Anche per questo problema la nostra soluzione è positiva, ed è riportata alla “questione n. 8” (che poi è nota anche come congettura di Legendre”) del lavoro su questo sito

“Congetture sui numeri primi ancora aperte...” al quale rimandiamo , e anche a “Soluzioni unificate per alcune congetture sul numero di primi in un certo intervallo” in sezione “Articoli sui numeri primi” La nostra dimostrazione di tale congettura ci ha

permesso recentemente di dimostrare anche la congettura di Andrica, in sezione “Articoli sui Numeri Primi “ e come conseguenza anche la congettura di Cramer – Shank (in sezione “Articoli sulla Teoria dei Numeri”).

3) (primi gemelli) esistono infiniti numeri primi p tali che $p+2$ è ancora primo?

Anche per questo problema rimando al suddetto lavoro “Congetture sui numeri aperte sui numeri primi”, quinta questione e relativi riferimenti), e alle considerazioni sulle PAP”Articoli sulle Progressioni” in questo stesso sito e in questo stesso articolo,

4) (congettura di Goldbach) ogni intero pari maggiore di 2 può essere scritto come somma di due numeri primi?

Anche per questo problema, rimando agli articoli di cui sopra, ed in particolare alla sezione “Articoli su Goldbach”, , oltre che alle relative considerazioni iniziali in questo stesso articolo.

Rimangono insoluti i due grossi problemi della fattorizzazione polinomiale (caso particolare del problema del millennio $P = NP$, si pensa che la fattorizzazione polinomiale sia in P se la RH fosse vera) risolvibile forse quando si conetteranno in qualche

modo i problemi additivi di cui sopra con quelli moltiplicativi, per esempio comprendendo meglio e bene i legami tra le somme di Goldbach e i prodotti di Goldbach, riguardanti le stesse coppie di numeri primi) e l'ipotesi di Riemann (qualche matematico pensa sia connessa alla fattorizzazione veloce, ma qualcun'altro nega invece tale connessione), che sarà risolta con ulteriori ricerche sulla funzione zeta e i suoi zeri sulla retta reale $\frac{1}{2}$, e sue possibili estensioni e generalizzazioni, o attraverso la dimostrazione di ipotesi RH equivalenti (Vedi "Sulle spalle dei giganti" già sul nostro sito, anche nella sezione "Articoli su Riemann").

Concludendo, i quattro principali problemi additivi sono stati da noi risolti o per lo meno avviati a soluzione, mentre per i problemi moltiplicativi (Fattorizzazione e Riemann) occorre attendere ancora eventuali e possibili connessioni sia con i suddetti problemi additivi e moltiplicativi.

Avendo ora o in seguito ben chiare queste relazioni e soluzioni, si potrebbero approfondire le ricerche future in tale direzione, per poter risolvere anche i due problemi moltiplicativi, uno per volta ma anche contemporaneamente;

in questo secondo caso solo se ci fosse una profonda connessione (ancora poco chiara) tra i due grossi problemi.

Una volta trovata (con o senza Riemann) una fattorizzazione polinomiale (cioè risolvibile in tempi polinomiali, il che riguarderebbe l'altro problema del millennio, P versus NP, almeno in questo caso), e quindi veloce (o almeno più veloce degli migliori algoritmi attuali (Lenstra, Pollard, Shor, crivello quadratico ecc.), si potrà riparlare anche di crittografia, ormai potenzialmente “violabile”, per sostituire gli attuali metodi crittografici (per esempio il sistema RSA) con metodi più efficaci: si pensa già ad una crittografia quantistica, ritenuta inattaccabile; con una crittografia alternativa già esiste, basata sulle curve ellittiche, ma con chiavi più corte rispetto alla crittografia RSA, e quindi anch'essa potenzialmente violabile.)

Il problema della fattorizzazione veloce potrà essere risolto con i futuri computer quantistici già in fase di sperimentazione - l'algoritmo di Shor richiede un computer quantistico - e che saranno sul mercato già tra qualche anno), velocissimi e potentissimi; ma i matematici dovrebbero risolvere tale problema

anche e soprattutto con la loro intelligenza, trovando un sistema veramente veloce di fattorizzazione basato su poche e semplici regole e relative formule polinomiali, e non soltanto sulla forza bruta dei computer, quantistici o no che siano...

GRUPPO ERATOSTENE

Caltanissetta 1.6.2010 (Data di revisione)

Riferimenti:

articoli vari sul nostro sito, nelle varie Sezioni, e già accennati nel corso del presente lavoro.